

(21) Application No 9226468.8

(22) Date of filing 18.07.1991

(30) Priority data

(31) 556890

(32) 23.07.1990

(33) US

(86) International application data

PCT/US91/05078 En 18.07.1991

(87) International publication data

WO92/02087 En 06.02.1992

(71) Applicant

Ericsson Ge Mobile Communications Inc

(Incorporated in the USA - Delaware)

1 Triangle Drive, Research Triangle Park, NC 27709,  
United States of America

(72) Inventor

Paul Wilkinson Dent

(74) Agent and/or Address for Service

Haseltine Lake &amp; Co

Hazlitt House, 28 Southampton Buildings,  
Chancery Lane, London, WC2A 1AT, United Kingdom(51) INT CL<sup>5</sup>

H04L 9/32

(52) UK CL (Edition L)

H4P PDCSA

U1S S2204 S2213

(56) Documents cited by ISA

US 4914696 A

US 4876740 A

US 4827507 A

US 4549308 A

(58) Field of search by ISA

US CL. 380/21,23,28,43,44,46,47,48,49,50, 455/33,  
375/107,110,112. 370/103,105,107, 379/59,60.

## (54) Authentication system for digital cellular communications

(57) A system for the authentication of mobile stations and base stations in a cellular communications network. The system includes an algorithm which generates not only a key dependent response to a random challenge, but also a temporary conversation key or call variable which may be used to encipher traffic in the network. To protect against clones in the network, the algorithm uses a rolling key which contains historical information. A bilateral authentication procedure may be used to update the rolling key and to generate a new conversation key.

